UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MINNESOTA

ROBERT KULLA, Derivatively on Behalf of TARGET CORPORATION, Plaintiff, v. GREGG W. STEINHAFEL, BETH M. JACOB, JAMES A. JOHNSON, SOLOMON D. TRUJILLO, ANNE M. MULCAHY, ROXANNE S. AUSTIN, CALVIN DARDEN, MARY E. MINNICK, DERICA W. RICE, JOHN G. STUMPF, DOUGLAS M. BAKER, JR., HENRIQUE DE CASTRO, and KENNETH L. SALAZAR, Defendants, -and- TARGET CORPORATION, a Minnesota corporation, Nominal Defendant.	Case No. _____ **VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT FOR BREACH OF FIDUCIARY DUTY AND WASTE OF CORPORATE ASSETS** **DEMAND FOR JURY TRIAL**

NATURE OF THE ACTION

1. This is a verified shareholder derivative action by plaintiff on behalf of nominal defendant Target Corporation ("Target" or the "Company") against certain of its officers and members of its Board of Directors (the "Board"). This action seeks to remedy defendants' violations of law, breaches of fiduciary duties, and waste of corporate assets that have caused substantial damages to the Company.

2. Target is the second largest general merchandise retailer in the United States. As part of its normal business practices, Target routinely collects its customers' personal and financial information, including credit and debit card numbers. Target assures its customers that it will protect this sensitive private information.

3. This action arises out of the Individual Defendants' (as defined herein) responsibility for the ***second biggest data breach in retail history***. In violation of its express promise to do so, and contrary to reasonable customer expectations, Target failed to take reasonable steps to maintain its customers' personal and financial information in a secure manner. As a result of Target's complete and utter lack of appropriate security measures, thieves were able to steal sensitive personal and financial data from as many of ***seventy million*** customers who shopped at Target between November 27, 2013 and December 15, 2013, the height of the 2013 holiday season. For many of these victims, identity thieves have already utilized their personal information to commit fraud and other crimes. For tens of millions of others, constant vigilance of their financial and personal records will be required to protect themselves from the threat of having their identity stolen.

4. The Individual Defendants aggravated the damage to consumers from the data breach by failing to provide adequate and prompt notice to consumers and conveying a false sense of security to affected customers. In particular, the Individual Defendants allowed Target to delay acknowledging the breach to the public until December 19, 2013, over ***three weeks*** after the data breach began. Worse, Target disclosed the data breach only after third-party reports already broke the news. Even then, Target concealed the full nature and scope of the data breach. In particular, Target initially reported that the data breach affected forty million people and assured those affected by the data breach that "***the issue has been identified and eliminated***," and that there was "***no indication that [personal identification number ("PIN")] numbers have been compromised***." Target further reassured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash."

5. Despite these statements to the contrary, just days after Target's initial disclosure of the data breach, news outlets began reporting that encrypted PIN data had been stolen during the breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its customers' PIN data had been compromised.

6. Then, on December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, on January 10, 2014, Target released another statement indicating that the breach was far more significant than the Company had been reporting. In particular, Target disclosed that ***seventy million***

customers may have been affected by the data breach, ***30 million*** more victims than Target previously reported.

7. The defendants' failures to implement any internal controls at Target designed to detect and prevent such a data breach, and then timely report it, have severely damaged Target. The Company's data breach is currently under investigation by the United States Secret Service ("Secret Service") and the Department of Justice ("DOJ"). Moreover, there are currently no less than ***nine*** class action lawsuits filed against Target on behalf of aggrieved customers. These class action lawsuits pose the risk of hundreds of millions of dollars in damages to the Company.

8. Plaintiff now brings this litigation on behalf of Target to rectify the conduct of the individuals bearing ultimate responsibility for the corporation's misconduct—the directors and senior management.

JURISDICTION AND VENUE

9. Jurisdiction is conferred by 28 U.S.C. §1332. Complete diversity among the parties exists and the amount in controversy exceeds $75,000, exclusive of interest and costs.

10. This Court has jurisdiction over each defendant named herein because each defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contacts with this District to render the exercise of jurisdiction by the District courts permissible under traditional notions of fair play and substantial justice.

11. Venue is proper in this Court in accordance with 28 U.S.C. §1391(a) because: (i) Target maintains its principal place of business in this District; (ii) one or more of the defendants either resides in or maintains executive offices in this District; (iii) a substantial portion of the transactions and wrongs complained of herein, including the defendants' primary participation in the wrongful acts detailed herein, and aiding and abetting and conspiracy in violation of fiduciary duties owed to Target, occurred in this District; and (iv) defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

THE PARTIES

Plaintiff

12. Plaintiff Robert Kulla was a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder. Plaintiff is a citizen of Pennsylvania.

Nominal Defendant

13. Nominal defendant Target is a Minnesota corporation with principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota. Accordingly, Target is a citizen of Minnesota. Target serves guests at 1,921 stores including 1,797 in the United States and 124 in Canada. The Company operates through three reportable segments: the U.S. Retail segment, which includes all of Target's U.S. merchandising operations; the U.S. Credit Card segment, which offers credit to qualified guests through its branded proprietary credit cards; and the Canadian segment which includes costs incurred in the U.S. and Canada related to the 2013 Canadian retail market entry.

Defendants

14. Defendant Gregg W. Steinhafel ("Steinhafel") is Target's Chief Executive Officer ("CEO") and has been since May 2008; President and has been since August 1999; Chairman of the Board and has been since February 2009; and a director and has been since 2007. Defendant Steinhafel has been employed by Target since 1979. Defendant Steinhafel knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Steinhafel the following compensation as an executive:

Fiscal Year	Salary	Stock Awards	Option Awards	Non-Equity Incentive Plan Compensation	Change in Pension Value and Nonqualified Deferred Compensation	Other Compensa-tion	Total
2012	$1,500,000	$5,285,245	$5,248,573	$2,880,000	$665,528	$5,068,118	$20,647,464

Defendant Steinhafel is a citizen of Minnesota.

15. Defendant Beth M. Jacob ("Jacob") is Target's Chief Information Officer and has been since July 2008 and Executive Vice President, Target Technology Services and has been since January 2010. Defendant Jacob was also Senior Vice President, Target Technology Services from July 2008 to January 2010 and Vice President, Guest Operations, Target Financial Services from August 2006 to July 2008. Defendant Jacob knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million

customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Jacob is a citizen of Minnesota.

16. Defendant James A. Johnson ("Johnson") is Target's Lead Independent Director and has been since at least April 2012 and a director and has been since 1996. Defendant Johnson is also a member of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Johnson knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Johnson the following compensation as a director:

Fiscal Year	Fees Paid in Cash	Stock Awards	Option Awards	Change in Pension Value and Nonqualified Deferred Compensation	Total
2012	$135,000	$90,055	$71,477	$13,174	$309,706

Defendant Johnson is a citizen of Washington, D.C.

17. Defendant Solomon D. Trujillo ("Trujillo") is a Target director and has been since 1994. Defendant Trujillo is also Chairman of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Trujillo knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Trujillo the following compensation as a director:

Fiscal Year	Fees Paid in Cash	Stock Awards	Option Awards	Change in Pension Value and Nonqualified Deferred Compensation	Total
2012	$105,000	$90,055	$71,477	$32,165	$298,697

Defendant Trujillo is a citizen of California.

18. Defendant Anne M. Mulcahy ("Mulcahy") is a Target director and has been since 1997. Defendant Mulcahy is also a member of Target's Audit Committee and has been since at least January 2014. Defendant Mulcahy knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Mulcahy the following compensation as a director:

Fiscal Year	Stock Awards	Total
2012	$275,003	$275,003

Defendant Mulcahy is a citizen of Connecticut.

19. Defendant Roxanne S. Austin ("Austin") is a Target director and has been since 2002. Defendant Austin is also Chairman of Target's Audit Committee and has been since at least April 2012. Defendant Austin knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Austin the following compensation as a director:

Fiscal Year	Fees Paid in Cash	Stock Awards	Option Awards	Total
2012	$120,000	$90,055	$71,477	$281,532

Defendant Austin is a citizen of California.

20. Defendant Calvin Darden ("Darden") is a Target director and has been since 2003. Defendant Darden is also a member of Target's Corporate Responsibility Committee and has been since at least January 2014. Defendant Darden knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Darden the following compensation as a director:

Fiscal Year	Fees Paid in Cash	Stock Awards	Option Awards	Total
2012	$90,000	$90,055	$71,477	$251,532

Defendant Darden is a citizen of Georgia.

21. Defendant Mary E. Minnick ("Minnick") is a Target director and has been since 2005. Defendant Minnick is also a member of Target's Audit Committee and Corporate Responsibility Committee and has been since at least April 2012. Defendant Minnick knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Minnick the following compensation as a director:

Fiscal Year	Stock Awards	Total
2012	$260,004	$260,004

Defendant Minnick is a citizen of the United Kingdom.

22. Defendant Derica W. Rice ("Rice") is a Target director and has been since 2007. Defendant Rice is also a member of Target's Audit Committee and has been since at least April 2012. Defendant Rice knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Rice the following compensation as a director:

Fiscal Year	Stock Awards	Total
2012	$260,004	$260,004

Defendant Rice is a citizen of Indiana.

23. Defendant John G. Stumpf ("Stumpf") is a Target director and has been since 2010. Defendant Stumpf was also a member of Target's Audit Committee from at least April 2012 to March 2013. Defendant Stumpf knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Stumpf the following compensation as a director:

Fiscal Year	Fees Paid in Cash	Stock Awards	Option Awards	Total
2012	$90,000	$90,055	$71,477	$251,532

Defendant Stumpf is a citizen of California.

24. Defendant Douglas M. Baker, Jr. ("Baker") is a Target director and has been since March 2013. Defendant Baker was also a member of Target's Audit

Committee from March 2013 to at least April 2013. Defendant Baker knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Baker is a citizen of Minnesota.

25. Defendant Henrique De Castro ("De Castro") is a Target director and has been since March 2013. Defendant De Castro is also a member of Target's Corporate Responsibility Committee and has been since March 2013. Defendant De Castro knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant De Castro is a citizen of California.

26. Defendant Kenneth L. Salazar ("Salazar") is a Target director and has been since July 2013. Defendant Salazar is also a member of Target's Corporate Responsibility Committee and has been since November 2013. Defendant Salazar knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Salazar is a citizen of Colorado.

27. The defendants identified in ¶¶14-15 are referred to herein as the "Officer Defendants." The defendants identified in ¶¶16-26 are referred to herein as the "Director

Defendants." Collectively, the defendants identified in ¶¶14-26 are referred to herein as the "Individual Defendants."

DUTIES OF THE INDIVIDUAL DEFENDANTS

Fiduciary Duties

28. By reason of their positions as officers and directors of the Company, each of the Individual Defendants owed and owe Target and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Target and not in furtherance of their personal interest or benefit.

29. To discharge their duties, the officers and directors of Target were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Target were required to, among other things:

(a) devise and maintain a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;

(b) ensure that the Company timely and accurately informed customers regarding any breach of their personal and financial information;

(c) conduct the affairs of the Company in an efficient, business-like manner in compliance with all applicable laws, rules, and regulations so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock; and

(d) remain informed as to how Target conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices.

Breaches of Duties

30. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as officers and directors of Target, the absence of good faith on their part, and a reckless disregard for their duties to the Company that the Individual Defendants were aware or reckless in not being aware posed a risk of serious injury to the Company.

31. The Individual Defendants, because of their positions of control and authority as officers and/or directors of Target, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein. The Individual Defendants also failed to prevent the other Individual Defendants from taking such illegal actions. As a result, and in addition to the damage the Company has already incurred, Target has expended, and will continue to expend, significant sums of money.

CONSPIRACY, AIDING AND ABETTING, AND CONCERTED ACTION

32. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct, and have acted in concert with and conspired with one another in furtherance of their common plan or design. In addition to the wrongful conduct herein alleged as giving rise to primary

liability, the Individual Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

33. The Individual Defendants engaged in a conspiracy, common enterprise, and/or common course of conduct. During this time, the Individual Defendants failed to timely and accurately inform customers regarding the full scope of the breach of their personal and financial information.

34. The purpose and effect of the Individual Defendants' conspiracy, common enterprise, and/or common course of conduct was, among other things, to disguise the Individual Defendants' violations of law, breaches of fiduciary duty, and waste of corporate assets; and to conceal adverse information concerning the Company's operations.

35. The Individual Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by allowing the Company to purposefully or recklessly conceal the scope of the data breach affecting at least seventy million customers. Because the actions described herein occurred under the authority of the Board, each of the Individual Defendants was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

36. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each Individual Defendant acted with knowledge of the primary wrongdoing, substantially

assisted in the accomplishment of that wrongdoing, and was aware of his or her overall contribution to and furtherance of the wrongdoing.

BACKGROUND OF THE COMPANY AND ITS PRIVACY POLICY

37. Target is the second largest general merchandise retailer in the United States. The Company operates 1,797 stores in the United States and 124 stores in Canada.

38. As stated in the Company's own "Privacy Policy," Target routinely collects personal information from its customers including a customer's name, mailing address, e-mail address, phone number, driver's license number, and credit/debit card number. In addition, when customers use their debit cards to make a purchase at Target, they are required to enter the PIN associated with their bank account. Target promises its customers that it will, among other things, "***maintain administrative, technical and physical safeguards to protect your personal information***. When we collect or transmit sensitive information such as a credit or debit card number, ***we use industry standard methods to protect that information***."

The Ramifications of Failing to Keep Customers' Data Secure Are Severe

39. Notwithstanding its promise and duties to protect its customers' sensitive personal and financial information, Target allowed the sensitive and private information of tens of millions of its customers to be stolen. Target's failure to protect its customers' sensitive personal and financial information exposes victims to identity theft. Identity theft occurs when someone wrongfully obtains another's personal information without their knowledge to commit theft or fraud.

40. Armed with a person's personal and financial information, identity thieves can encode the victim's account information onto a different card with a magnetic strip creating a counterfeit card that can be used to make fraudulent purchases. With the addition of a victim's PIN, a thief can use the counterfeit card to withdraw money from that person's bank account.

41. Identity thieves can cause further damage to their victims by using personal information to open new credit and utility accounts, receive medical treatment on their health insurance, or even obtain a driver's license. Once a person's identity has been stolen, reporting, identifying, monitoring, and repairing the victim's credit is a cumbersome, expensive, and time-consuming process. In addition to the frustration of having to identify and close affected accounts, correct information in their credit reports, victims of identity theft often incur costs associated with defending themselves against civil litigation brought by creditors. Victims also suffer the burden of having difficulty obtaining new credit. Moreover, victims of identity theft must monitor their credit reports for future inaccuracies as fraudulent use of stolen personal information may persist for several years.

42. Annual monetary losses from identity theft are in the billions of dollars. According to The President's Identity Theft Task Force Report dated October 21, 2008, on identity theft produced in 2008:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, ... individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for

> example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

43. The significant impact identity theft can have on consumers and the extreme financial ramification the failure to secure personal information can cause has led to the enactment of numerous privacy-related laws aimed toward protecting consumer information and disclosure requirements, including, for example: (i) Gramm-Leach-Bliley Act; (ii) Fair Credit Reporting Act; (iii) Fair and Accurate Credit Transactions Act; (iv) Federal Trade Commission Act, 15 U.S.C. §§41-58; (v) Driver's Privacy Protection Act; (vi) Health Insurance Portability and Accountability Act; (vii) The Privacy Act of 1974; (viii) Social Security Act Amendments of 1990; (ix) E-Government Act of 2002; and (x) Federal Information Security Management Act of 2002.

44. Moreover, the recent wave of cyber-attacks striking American corporations prompted warnings from federal officials, including one issued in May 2013 by the Department of Homeland Security. In particular, the warning was issued by an agency called ICS-Cert, which monitors attacks on computer systems that run industrial processes. The warning stated that the government was "highly concerned about hostility against critical infrastructure organizations."

45. The Individual Defendants were fully aware of the risk of a potential data breach. On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, publicly disclosed a white paper[1] titled "Point-of-Sale Vulnerabilities" (the "White Paper") warning Target about the possibility of a point-of-sale data breach. The White Paper used Target as an example of the potential ramifications of a point-of-sale data breach at a major retailer and estimated that as many as fifty-eight million card accounts could be compromised if Target's point-of-sale system was compromised.

46. Moreover, the Individual Defendants were fully aware of the ramifications of failing to keep customers' data secure and knew that the Company could be subject to costly government enforcement actions and private litigation. As stated in the risk disclosures in the Company's Annual Report on Form 10-K filed with the U.S. Securities and Exchange Commission ("SEC") on March 20, 2013:

> ***If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation***. In addition, ***our guests could lose confidence in our ability to protect their personal information***, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. ***The loss of confidence from a significant data security breach involving team members could hurt our reputation***, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.

[1] A white paper is an authoritative report or guide helping readers to understand an issue, solve a problem, or make a decision. White papers are used in two main spheres: government and business-to-business marketing.

THE INDIVIDUAL DEFENDANTS' FAILURE TO PROTECT CUSTOMERS' PERSONAL INFORMATION LEADS TO RECORD-SETTING DATA BREACH

47. Target's data breach compromised seventy million customers' personal and financial data. Within days of the breach, millions of affected customers' financial and personal information was being sold on the black-market. Moreover, bank cards that had only been used at Target were found to have been used to make unauthorized purchases at Target stores.

48. News of the data breach first broke out on December 18, 2013, when KrebsOnSecurity.com, a website dedicated to reporting cybercrime, published an article indicating the occurrence of a massive data breach at Target stores. According to the report, Target was investigating the possible theft of millions of customer credit card and debit card records beginning November 27, 2013, and extending as far as December 15, 2013. The breach was thought to have occurred when thieves accessed the Company's customers' personal and financial data by breaking into Target's point-of-sale system.

Target's Initial Reports of the Data Breach Provide False Assurances to Customers

49. Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. In so doing, the Individual Defendants aggravated the damage to affected customers.

50. Only after news of the data breach spread did the Company even mention the credit card attack. On December 19, 2013, over three weeks after the data breach

began, Target finally acknowledged the breach to the public. The Company issued a brief statement in which it confirmed that it had been aware of unauthorized access to certain customers' credit and debit card data at the Company's U.S. stores. According to the statement, "[a]pproximately ***40 million*** credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013." In a separate statement issued that same day, Target conceded that customer data compromised in the data breach "included customer name, credit or debit card number, and the card's expiration date and CVV [card verification value]."

51. On December 20, 2013, in a rushed attempt to contain and minimize the perceived impact of the data breach, Target professed to "have worked swiftly to ***resolve the incident***" and concluded that, "there is ***no indication that PIN numbers have been compromised*** on affected bank issued PIN debit cards or Target debit cards." Target assured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash." That same day, Target issued a press release announcing that "***the issue has been identified and eliminated***" and that the Company would provide free credit monitoring services to affected customers. In an effort to restore confidence in the Company, Target offered to extend its employees' discount of 10% to all customers who shopped in Target stores on December 21 and 22, 2013.

52. Despite Target's attempts to dispel customers' concerns, news began to emerge that credit and debit card information stolen from Target had begun to appear for sale online. According to an article by KrebsOnSecurity.com, customer account information stolen from Target was being sold on the black market "in batches of one

million cards" and fraudulent purchase activity had begun being reported by issuing banks.

53. As the growing scope of the breach continued to be revealed, Target confirmed on December 23, 2013, that the Secret Service and the DOJ decided to participate in the investigation into the breach. In addition, the Attorneys General from Massachusetts, New York, Connecticut, and South Dakota also began looking into the data breach.

54. The following day, *Reuters* reported that, despite prior statements by Target to the contrary, encrypted PIN data had been stolen during the original breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its customers' PIN data had been compromised. As stated in defendant Steinhafel's letter to Target's customers published shortly after the Company's initial acknowledgment of the breach:

> We want you to know a few important things:
>
> - The unauthorized access took place in U.S. Target stores between Nov. 27 and Dec. 15, 2013. Canadian stores and target.com were not affected.
>
> - ***Even if you shopped at Target during this time frame, it doesn't mean you are a victim of fraud. In fact, in other similar situations, there are typically low levels of actual fraud***.
>
> - There is ***no indication that PIN numbers have been compromised*** on affected bank issued PIN debit cards or Target debit cards. ***Someone cannot visit an ATM with a fraudulent debit card and withdraw cash***.

- You will not be responsible for fraudulent charges—either your bank or Target have that responsibility.

The Full Scope of the Data Breach Is Revealed

55. Then, on December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, in yet another glaring indication that the Company had not yet "resolved" the matter, Target released a statement indicating that the breach was far more significant than the Company had been reporting. On January 10, 2014, Target disclosed that ***70 million*** customers may have been affected by the data breach, thirty million more victims that Target previously reported.

The Individual Defendants Knew or Should Have Known that the Company's Customers Were Vulnerable to Attack Yet Failed to Implement Appropriate Security Measures

56. Target recognizes that its customers' personal and financial information is highly sensitive and must be protected. Moreover, as discussed above, Target promises its customers that it will "maintain administrative, technical and physical safeguards to protect [customers'] information" and "use industry standard methods to protect that information." Target's Privacy Policy states:

> ***We maintain administrative, technical and physical safeguards to protect your personal information***. When we collect or transmit sensitive information such as a credit or debit card number, ***we use industry standard methods*** to protect that information.

57. The PCI Data Security Standard ("PCI") is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of twelve general requirements including:

1. Install and maintain a firewall configuration to protect cardholder data;

2. Do not use vendor-supplied defaults for system passwords and other security parameters;

3. Protect stored cardholder data;

4. Encrypt transmission of cardholder data across public networks;

5. Use and regularly update anti-virus software or programs;

6. Develop and maintain secure systems and applications;

7. Restrict access to cardholder data by business need to know;

8. Assign a unique ID to each person with computer access;

9. Restrict physical access to cardholder data;

10. Track and monitor all access to network resources and cardholder data;

11. Regularly test security systems and processes; and

12. Maintain a policy that addresses information security for all personnel.

58. On December 23, 2013, *USA Today* reported that Target was likely not complying with the PCI. The article stated:

> Target's massive databreach took place just a few weeks before a set of payment card industry standards – known as PCI DSS 3.0 – were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.
>
> CyberTruth: What does this latest databreach tell us about the efficacy of PCI?
>
> Aceto: We can't say definitely that this breach is a failure of Target's PCI compliance, but ***based on what Target has said, it's very hard to believe that they were even PCI 2.0 compliant at the time of the breach***.

> A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?
>
> One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring involves file integrity checks and changes to critical systems files. What's more – the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.
>
> Unusual activity isn't always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions – like busy shopping days Black Friday and Cyber Monday, on which the breach occurred – detract from the monitoring effort.

59. The Individual Defendants knew or should have known that the Company's less than industry-standard security systems and unreasonably vulnerable technologies would render its customers an aim of attacks by third-parties. The Individual Defendants, however, failed to take corrective measures to update its systems and technologies. Among Target's deficiencies in this respect were its failure to maintain adequate backups and/or redundant systems; failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency; and failure to provide prompt and adequate warnings of security breaches.

DAMAGES TO TARGET

60. As a result of the Individual Defendants' improprieties, thieves were able to steal sensitive personal and financial data from at least seventy million customers. Target's failure to protect its customers' personal and financial information has damaged its reputation with its customer base. In addition to price, Target's current and potential customers consider a company's ability to protect their personal and financial information

when choosing where to shop. Customers are less likely to shop at stores that cannot be trusted to safeguard their sensitive private information. The impact of the breach on the Company's bottom line has already begun to be revealed. In particular, the Company has experienced "meaningfully weaker-than-expected sales since the announcement," which lead the Company to cut its fourth quarter 2013 adjusted earnings per share ("EPS") of $1.20 to $1.30, compared to previous guidance of $1.50 to $1.60.

61. Further, as a direct and proximate result of the Individual Defendants' actions, Target has expended, and will continue to expend, significant sums of money. Such expenditures include, but are not limited to:

(a) costs incurred from defending and paying any settlement in the numerous consumer class actions filed against the Company;

(b) costs incurred from the Secret Service and DOJ investigations into the data breach, including, but not limited to, liability for any potential fines;

(c) costs incurred from the Company's internal investigation into the data breach, including, but not limited to, expense for legal, investigative, and consulting fees;

(d) costs incurred from expenses and capital investments for remediation activities;

(e) costs incurred from notifying customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges;

(f) costs incurred from Target fulfilling its promise to provide free credit monitoring to victims of the data breach;

(g) loss of revenue and profit resulting from Target's offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores; and

(h) costs incurred from compensation and benefits paid to the defendants who have breached their duties to Target.

DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS

62. Plaintiff brings this action derivatively in the right and for the benefit of Target to redress injuries suffered, and to be suffered, by Target as a direct result of breaches of fiduciary duty and waste of corporate assets, as well as the aiding and abetting thereof, by the Individual Defendants. Target is named as a nominal defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

63. Plaintiff will adequately and fairly represent the interests of Target in enforcing and prosecuting its rights.

64. Plaintiff was a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder.

65. The current Board of Target consists of the following twelve individuals: defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo. Plaintiff has not made any demand on the present Board

to institute this action because such a demand would be a futile, wasteful, and useless act, as set forth below.

Demand Is Excused Because the Director Defendants' Conduct Is Not a Valid Exercise of Business Judgment

66. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo, constituting the Company's entire current Board, caused the Company to disseminate improper, materially false and misleading public statements concerning, among other things, the true nature and extent of the data breach. Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. The Company's public disclosures concerning the data breach were improper because: (i) they were untimely and only released after third-party organizations began spreading the news; (ii) they understated the scope of the affected victims by thirty million people; and (iii) they diminished the severity of the harm to customers by failing to disclose that PINs were compromised. Each member of the Board knew or should have known that the improper statements did not timely, fairly, accurately, or truthfully convey the scope of the data breach. In addition, when deciding whether to approve statements to be publicly disseminated, each member of the Board was bound by the duty of care to inform himself or herself of all reasonably-available material information. Information concerning the nature and extent of the data breach was both reasonably available and material to

members of the Board. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo's conduct can in no way be considered a valid exercise of business judgment. Accordingly, demand on the Board is excused.

Demand Is Excused Because the Entire Board Faces a Substantial Likelihood of Liability for Their Misconduct

67. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo, all twelve members of the current Board, are disqualified from fairly evaluating the derivative claims, let alone vigorously prosecuting them, because they are each responsible for damages suffered by Target as a result of the Company's massive data breach. The Board was responsible for ensuring that internal controls were implemented and maintained to protect the Company's customers' personal and financial information. Instead, the Board failed to implement any internal controls to detect or prevent such a data breach from occurring. Despite each Individual Defendant's responsibility for "maintain[ing] administrative, technical, and physical safeguards to protect [customers'] personal information," defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo took no action to ensure such protection. These defendants' complete and utter failure to establish a system of appropriate internal controls and compliance measures is a breach of their duty of loyalty. As such, the entire Board faces a substantial likelihood of liability, rendering demand upon them futile.

68. Further, defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo face a substantial likelihood of liability due to their failure to provide adequate and prompt notice to consumers and because they conveyed a false sense of security to customers affected by the data breach. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo breached their duty of loyalty by causing the Company to disseminate the improper public statements discussed herein. Accordingly, all the Board members face a substantial likelihood of liability, further rendering demand upon them futile.

69. Any suit by the current directors of Target to remedy these wrongs would expose Target to liability in the numerous pending consumer class actions lawsuits. There are currently no less than nine consumer class actions filed against the Company as a result of the data breach. These class actions allege various claims, including, but not limited to, negligence, breach of contract, and violation of state privacy laws. If the Board elects for the Company to press forward with its right of action against any of the members of the Board in this action, then Target's efforts would compromise its defense of the pending consumer class actions. Accordingly, demand on the Board is excused.

70. The acts complained of constitute violations of the fiduciary duties owed by Target's officers and directors and these acts are incapable of ratification.

71. Target has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Individual Defendants and current Board have not filed any lawsuits against themselves or others who were responsible for that

wrongful conduct to attempt to recover for Target any part of the damages Target suffered and will suffer thereby.

72. Plaintiff has not made any demand on the other shareholders of Target to institute this action since such demand would be a futile and useless act for at least the following reasons:

(a) Target is a publicly held company with over 632 million shares outstanding and thousands of shareholders;

(b) making demand on such a number of shareholders would be impossible for plaintiff who has no way of finding out the names, addresses, or phone numbers of shareholders; and

(c) making demand on all shareholders would force plaintiff to incur excessive expenses, assuming all shareholders could be individually identified.

COUNT I

Against the Individual Defendants for Breach of Fiduciary Duty

73. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

74. As alleged in detail herein, the Individual Defendants, by reason of their positions as officers and directors of Target and because of their ability to control the business and corporate affairs of Target, owed to Target fiduciary obligations of due care and loyalty, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner.

75. The Officer Defendants breached their duty of loyalty by knowingly, recklessly, or with gross negligence: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the full scope of the data breach, which affected at least seventy million customers.

76. The Director Defendants breached their duty of loyalty by knowingly or recklessly: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the full scope of the data breach, which affected at least seventy million customers.

77. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Target has sustained significant damages, as alleged herein. As a result of the misconduct alleged herein, these defendants are liable to the Company.

78. Plaintiff, on behalf of Target, has no adequate remedy at law.

COUNT II

Against all Individual Defendants for Waste of Corporate Assets

79. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

80. The wrongful conduct alleged included the failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information. Under the Individual Defendants' purview, Target's customers became the victims of the second biggest data breach in retail history. The Company already incurred substantial costs in investigating the data breach and cooperating with

various government investigations. In addition, the Company lost revenue and profit due to its offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores after the data breach. The Company will continue to incur substantial costs from the numerous consumer class actions filed against it.

81. Further, the Individual Defendants caused Target to waste its assets by paying improper compensation and bonuses to certain of its executive officers and directors that breached their fiduciary duty.

82. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

83. Plaintiff, on behalf of Target, has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, plaintiff, on behalf of Target, demands judgment as follows:

A. Against the Individual Defendants and in favor of the Company for the amount of damages sustained by the Company as a result of the Individual Defendants' breach of fiduciary duty, waste of corporate assets, and aiding and abetting breaches of fiduciary duties;

B. Directing Target to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for shareholder vote, resolutions for amendments to the Company's By-Laws or Articles of Incorporation, and taking such

other action as may be necessary to place before shareholders for a vote of the following Corporate Governance Policies:

1. a proposal to strengthen the Company's controls over its customers' personal and financial information;

2. a proposal to create a committee tasked with monitoring the Company's security measures;

3. a proposal to strengthen the Company's disclosure controls;

4. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater shareholder input into the policies and guidelines of the Board; and

5. a provision to permit the shareholders of Target to nominate at least three candidates for election to the Board;

C. Awarding to Target restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;

D. Awarding plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs and expenses; and

E. Granting such other and further equitable relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury.

Dated: January 21, 2014

WALSH LAW FIRM

/s/Christopher R. Walsh

CHRISTOPHER R. WALSH (#199813)
Attorney at Law
Fifth Street Towers
100 South Fifth Street, Suite 1025
Minneapolis, MN 55402
Telephone: 612-767-7500
Facsimile: 612-677-9300
walshlawfirm@comcast.net

ROBBINS ARROYO LLP
BRIAN J. ROBBINS
FELIPE J. ARROYO
SHANE P. SANDERS
600 B Street, Suite 1900
San Diego, CA 92101
Telephone: (619) 525-3990
Facsimile: (619) 525-3991
brobbins@robbinsarroyo.com
farroyo@robbinsarroyo.com
ssanders@robbinsarroyo.

Attorneys for Plaintiff

922652

VERIFICATION

I, Robert Kulla, hereby declare as follows:

I am the plaintiff in the within entitled action. I have read the Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets. Based upon discussions with and reliance upon my counsel, and as to those facts of which I have personal knowledge, the Complaint is true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Signed and Accepted:

Dated: 1/20/2014

ROBERT KULLA